



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/675,159	09/29/2003	Richard Braun	073897.0145	5546
5073	7590	10/04/2006	EXAMINER	
BAKER BOTT'S L.L.P. 2001 ROSS AVENUE SUITE 600 DALLAS, TX 75201-2980				MABINI, MARVIN
ART UNIT		PAPER NUMBER		
		2153		

DATE MAILED: 10/04/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	10/675,159	BRAUN ET AL.
	Examiner	Art Unit
	Marvin Mabini	2153

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).

Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) Responsive to communication(s) filed on 29 September 2003.

2a) This action is **FINAL**. 2b) This action is non-final.

3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) Claim(s) 1-27 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) Claim(s) _____ is/are allowed.

6) Claim(s) 1-27 is/are rejected.

7) Claim(s) _____ is/are objected to.

8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) The specification is objected to by the Examiner.

10) The drawing(s) filed on 29 September 2003 is/are: a) accepted or b) objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a) All b) Some * c) None of:

1. Certified copies of the priority documents have been received.
2. Certified copies of the priority documents have been received in Application No. _____.
3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) Notice of References Cited (PTO-892)

2) Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) Information Disclosure Statement(s) (PTO/SB/08)
 Paper No(s)/Mail Date 20030929.

4) Interview Summary (PTO-413)
 Paper No(s)/Mail Date. _____.

5) Notice of Informal Patent Application

6) Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 112

1. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.
2. Claim 6 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 6 recites the limitation "the remote user device" in line 2. There is insufficient antecedent basis for this limitation in the claims. Should the phrase "the remote user device", in claim 6 line 2, read "a remote user device?

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claims 1-7, 9-12, 13-19, and 21-27 are rejected under 35 U.S.C. 102(b) as being anticipated by US Patent 5774650 to Chapman et al. (hereinafter Chapman).

As per claim 1 and 25 Chapman discloses a method for using a utility (see access control program – Chapman column 6 lines 13-19; the program allows a permitted user to make administrative configuration changes) at an end user device

(see systems 2,4,6,8 - Chapman column 3 lines 20-22; the utility resides in the systems), comprising:

- Assigning an elevated access right (see privilege user – Chapman column 4 lines 1-4) to a remote (see remote – Chapman column 3 lines 39-43) user identifier (see user account – Chapman column 4 lines 14-15; also see user number zero – Chapman column 4 lines 39-40; user with the identifier zero refers to having an elevated access) and a limited access right to an end user identifier (see normal user – Chapman column 4 lines 1-4; also see user account – Chapman column 4 lines 14-15), the limited access right operable to prevent access to the utility at the end user device (see unauthorized users to be denied access –Chapman column 5 lines 6-10);
- accessing the utility at the end user device using the remote user identifier (access control program – Chapman column 4 lines 2-4), the utility operable to allow the remote user identifier (see provide for privilege user – Chapman column 4 lines 4-6);to select an administrative tool at the end user device (see command line – Chapman column 6 lines 13-19; command line is the administrative tool used by a user with proper access rights to change or configure the end user system)
- launching the administrative tool according to the elevated access right while maintaining the limited access right of the end user identifier (see check and create temporarily unauthorized users – Chapman column 6 lines 56-57; note that the user with elevated access rights has full privileges to the system's

command line, while unauthorized user do not have access to the system's command line; therefore the administrative tool, in the Chapman reference this is referred to as the command line, is launched by the user with elevated access right while maintaining the limited access of the other user); and

- performing at least one administrative task at the end user device using the administrative tool (see entering command – Chapman column 6 lines 20-22).

As per claims 2 and 14 Chapman discloses, wherein assigning an elevated access right (see privilege user – Chapman column 4 lines 1-4) to a remote user identifier and a limited access right to an end user identifier further comprises:

- setting up at a network directory a remote user profile for the remote user identifier, the remote user profile associating the remote user identifier with the elevated access right (see Figure 2 and user account file – Chapman column 4 lines 23-26; also see super user denoted by user number zero – Chapman column 4 line 39-40); and
- setting up at the network directory an end user profile, the end user profile associating the end user identifier with the limited access right (see Figure 2 and user account file – Chapman column 4 lines 23-26; also see create definition – Chapman line 56-57; the definition corresponds to the user name in the user account profile, and based on this the user has limited access right since the definition states the unauthorized users).

As per claim 3 and 15 Chapman discloses, wherein accessing the utility at the end user device using the remote user identifier further comprises receiving the remote user identifier (see login – Chapman column 5 lines 22-28; the username that is typed in is the remote user identifier); authenticating the remote user identifier using a network directory, the network directory comprising a profile associating the remote user identifier with the elevated access right (see authenticating and access rights – see Chapman column 5 lines 30-41; note that the account details is obtained from the user account file shown in figure 2); and granting access to the utility using the elevated access right (see invoke access control program and check that user is privilege to do so – Chapman column 6 lines 20-25).

As per claims 4,10,16 and 22 Chapman discloses, establishing a remote connection using a remote control module at a remote user device (see session can be opened with the remote system 2 using protocol – Chapman column 5 lines 18-22).

As per claims 5,11, 17 and 23 Chapman discloses, detecting a break in the remote Connection (see logging off – see Chapman column 7 lines 14-17; logging off breaks remote connection); and closing at least one process (see terminating all processes – Chapman column 7 lines 16-17), the at least one process corresponding to

the administrative tool used to perform the administrative task (see exit access control program – Chapman column 7 lines 28-30).

As per claims 6,12,18 and 24 as best understood, Chapman discloses, wherein the remote user identifier is associated with the remote user device (see superuser – Chapman column 4 lines 39-40), the remote user device (see Chapman figure 1 block 12) located at a separate location (see other remote terminals – Chapman column 3 lines 39-43; note that the terminals are stated as remote therefore separate from the RISC System which corresponds to figure 1 block 2) from the end user device (see Chapman figure 1 block 2).

As per claims 7 and 19 Chapman discloses, wherein the administrative task comprises operations that affect the settings of the end user device (command line arguments supplied – Chapman column 6 lines 29-36; the command line arguments are the administrative tasks that will affect settings at the end user device, which includes restricting access).

As per claims 9, 21 and 26, Chapman discloses a method and software of elevating an access right at an end user device (see remote – Chapman column 3 lines 39-43), comprising:

- receiving an authentication message from a network in response to a login request from a remote user identifier (see authenticating and access rights – see

Chapman column 5 lines 30-41; note that the account details is obtained from the user account file shown in figure 2), the authentication message operable to inform if the remote user identifier is associated with an elevated access right, the elevated access right operable to allow access to an administrative tool at the end user device (see invoke access control program and check that user is privilege to do so – Chapman column 6 lines 20-25).;

- generating an elevated access layer using the elevated access right, the elevated access layer operable to: initiate an administrative tool at the end user device (see invoke access control program and check that user is privilege to do so – Chapman column 6 lines 20-25); and elevate the access right of the remote user identifier according to the elevated access right (see privilege user – Chapman column 4 lines 1-4);
- launching the administrative tool using the elevated access layer (see entering command – Chapman column 6 lines 20-22); and
- processing at least one administrative task at the end user device using the administrative tool while maintaining an end user identifier logged into the network with a limited access right (see check and create temporarily unauthorized users – Chapman column 6 lines 56-57; note that the user with elevated access rights has full privileges to the system's command line, while unauthorized user do not have access to the system's command line; therefore the administrative tool, in the Chapman reference this is the command line, is launched by the user with elevated access right while maintaining the limited

access of the other user), the limited access right operable to prevent access to the administrative tool at the end user device (see Figure 2 and user account file – Chapman column 4 lines 23-26; also see create definition - Chapman line 56-57; the definition corresponds to the user name in the user account profile, and based on this the user has limited access right since the definition states the unauthorized users).

As per claim 13, Chapman discloses, a system for elevating access rights of a remote user, comprising:

- a network directory operable to assign an elevated access right to a remote user identifier and a limited access right to an end user identifier (see Figure 2 and user account file – Chapman column 4 lines 23-26; also see super user denoted by user number zero – Chapman column 4 line 39-40);
- a utility stored (access control program – Chapman column 4 lines 2-4) at an end user device and operable to:
- launch the administrative tool according to the elevated access right while maintaining the limited access right of the end user identifier, the limited access right operable to prevent access to the utility at an end user device (see check and create temporarily unauthorized users – Chapman column 6 lines 56-57; note that the user with elevated access rights has full privileges to the system's command line, while unauthorized user do not have access to the system's command line; therefore the administrative tool, in the Chapman

reference this is the command line, is launched by the user with elevated access right while maintaining the limited access of the other user); and

- perform at least one administrative task at the end user device using the administrative tool (see entering command – Chapman column 6 lines 20-22); and
- a remote (see remote – Chapman column 3 lines 39-43) user device (see Chapman figure 1 block 12) operable to access the utility at the end user (access control program – Chapman column 4 lines 2-4) device using the remote user identifier (see provide for privilege user – Chapman column 4 lines 4-6) in order to perform the at least one administrative task at the end user device (see command line – Chapman column 6 lines 13-19; this command line is the administrative tool used by a user with proper access rights to change or configure the end user system).

As per claim 27, Chapman discloses,

A method of elevating an access right at an end user device, comprising:

- receiving an authentication message from a network in response to a login request from a remote user identifier (see authenticating and access rights – see Chapman column 5 lines 30-41; note that the account details is obtained from the user account file shown in figure 2), the authentication message operable to inform if the remote user identifier is associated with an elevated access right, the elevated access right operable to allow access to an administrative tool at the

end user device, (see invoke access control program and check that user is privilege to do so – Chapman column 6 lines 20-25).

- the remote user identifier associated with a remote user device (see superuser – Chapman column 4 lines 39-40), the remote user device (see Chapman figure 1 block 12) being at a separate location from the end user device (see Chapman figure 1 block 2);
- generating an elevated access layer using the elevated access right, the elevated access layer operable to: initiate an administrative tool at the end user device (see invoke access control program and check that user is privilege to do so – Chapman column 6 lines 20-25); and elevate the access right of the remote user identifier according to the elevated access right (see privilege user – Chapman column 4 lines 1-4);
- launching the administrative tool using the elevated access layer (see entering command – Chapman column 6 lines 20-22); and
- processing at least one administrative task at the end user device using the administrative tool while maintaining an end user identifier logged into the network with a limited access right (see check and create temporarily unauthorized users – Chapman column 6 lines 56-57; note that the user with elevated access rights has full privileges to the system's command line, while unauthorized user do not have access to the system's command line; therefore the administrative tool, in the Chapman reference this is the command line, is launched by the user with elevated access right while maintaining the limited

access of the other user), the limited access right operable to prevent access to the administrative tool at the end user device (see Figure 2 and user account file – Chapman column 4 lines 23-26; also see create definition -Chapman line 56-57; the definition corresponds to the user name in the user account profile, and based on this the user has limited access right since the definition states the unauthorized users);

- detecting a remote connection from the remote user device, the remote connection operable to access the end user device using a remote control module at the remote user device (see session can be opened with the remote system 2 using protocol – Chapman column 5 lines 18-22); and
- discontinuing (see logging off – see Chapman column 7 lines 14-17; logging off breaks remote connection) at least one process (see terminating all processes – Chapman column 7 lines 16-17), associated with the administrative tool upon detecting a break in the remote connection (see exit access control program – Chapman column 7 lines 28-30).

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. Claims 8 and 20 is rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 5774650 to Chapman et al. (hereinafter Chapman) in view of US Patent 6289378 to Meyer et al (hereinafter Meyer).

As per claim 8 and 20, Chapman discloses all the limitations of parent claims 1 and 13 from which claims 8 and 20 depend, respectively (see above 102 rejections for claim 1 and 13).

Chapman does not disclose expressly wherein the end user device comprises an operating system selected from a group consisting of WINDOWS XP and WINDOWS 2000.

The concept of using Windows as operating system is well known in the art as illustrated by Meyer which teaches an end user device comprises an operating system selected from a group consisting of WINDOWS XP and WINDOWS 2000 (see Windows – column 4 lines 61-64).

Meyer and Chapman are analogous art because both have a similar problem solving area, which is to restrict access to users based on the definitions of authorized users. At the time of the invention, it would have been obvious to a person of ordinary skill in the art to modify the system of Chapman with a user device comprises an operating system selected from a group consisting of windows such as disclosed by Meyer et al. The motivation is to provide a platform independent system so as to incorporate comparable devices that are widely used, such as a device that runs on the Windows environment.

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

"Windows 2000 Centralized Management", White Paper, Microsoft Windows 2000 Server, 2000, 16 pages, teaches active directory, remote desktop, and allowing permissions and group policy settings to access objects and domain resources.

US Patent 6470339 to Karp et al, teaches providing access control to resources.

US Patent 6775781 to Phillips et al, teaches a network where there is an administrative privileges that can initiate administrative function.

US Patent 6308274 to Swift, teaches a process associated with a restricted token, where a token can grant or deny access.

US Patent Application Publication 2002/0112038 teaches a remote configuration utility, the utility includes a control console.

US Patent 6886100 to Harrah et al, teaches delegating tools to a user based on a role. The tool provides access for performing a task, and the role is authorized.

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Marvin Mabini whose telephone number is 571-270-1142. The examiner can normally be reached on Monday-Friday 9AM-5PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Glenton B. Burgess can be reached on 571-272-3949. The fax phone

number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

MM/



GLENTON B. BURGESS
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100